Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid

Rev. 0.0.2, 09 September 2020

Cisco Systems, Inc.

Total pages: 29

Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE) via pxGrid

Rev. 0.0.2, 09 September 2020

Owner: **Cisco IoT**

Author: **Juliette Maffet**

Cisco Systems, Inc.

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent. A printed copy of this document is considered uncontrolled. Refer to the online version for the latest revision.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Contents

1 About this documentation

1.1 Document purpose

This manual provides important information on the required configurations to enable the integration of Cisco Cyber Vision with Cisco ISE via pxGrid.

This manual takes into consideration the Cisco Cyber Vision application with the highest license level (Protect & Respond) and involves all available users roles (from full rights to read-only).

This manual is applicable to **system version 3.1.1**.

1.2 Warnings and notices

This manual contains notices you have to observe to ensure your personal safety as well as to prevent damage to property.

The notices referring to your personal safety and to your property damage are highlighted in the manual by a safety alert symbol described below. These notices are graded according to the degree of danger.

WARNING

Indicates risks that involve industrial network safety or production failure that could possibly result in personal injury or severe property damage if proper precautions are not taken.

IMPORTANT

Indicates risks that could involve property or Cisco equipment damage and minor personal injury if proper precautions are not taken.

Note

Indicates important information on the product described in the documentation to which attention should be paid.

2 Purpose

The following procedures explain how to:

- Start and configure ISE to receive Cisco Cyber Vision data.
- Configure the pxGrid link between Cisco Cyber Vision and ISE.
- Test the link.
- Troubleshoot the link.

3 Requirements

Before starting the procedures described in this document, make sure you've collected the following elements:

ISE

- The IP address for ISE administration.
- The IP address of the pxGrid node.
- The FQDN of the pxGrid node.
- An administration account name and password.

Cisco Cyber Vision

- The IP address of the Center.
- The FQDN (Fully Qualified Domain Name) of the Center.
- A Cisco Cyber Vision Administrator access.

4 Introduction

The link between Cisco Cyber Vision and ISE is aimed to create endpoints in ISE based on Cisco Cyber Vision's components. pxGrid is used to publish discovered components as endpoints in ISE.

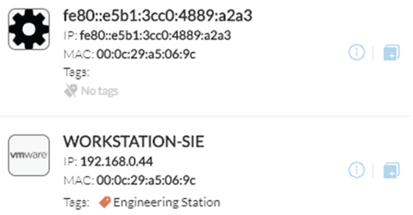
Cisco Cyber Vision components are created and maintained in ISE with the following rules:

- Component aggregation based on MAC addresses.
- Refresh of Cisco Cyber Vision components' properties as they are updated.
- A list of properties is sent from Cisco Cyber Vision to ISE. Some are predefined in ISE, others need to be created manually.

4.1 MAC aggregation

When endpoints in ISE are the equivalent of components in Cisco Cyber Vision, they are handled differently. In fact, ISE endpoints have a single MAC address and are listed as such, whereas in Cisco Cyber Vision several components can have the same MAC address and/or the same IP address and are aggregated in one component.

Example:



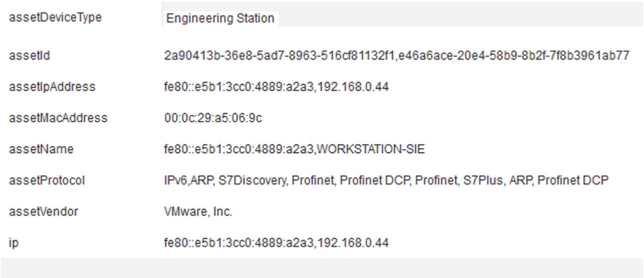
fe80::e5b1:3cc0:4889:a2a3
IP: fe80::e5b1:3cc0:4889:a2a3
MAC: 00:0c:29:a5:06:9c
Tags:
No tags

WORKSTATION-SIE
IP: 192.168.0.44
MAC: 00:0c:29:a5:06:9c
Tags: Engineering Station

These components represent a virtual machine with two IP addresses (an IPV4 and an IPV6) on the same MAC address.

In this case, Cisco Cyber Vision sends to ISE an aggregated component based on the MAC address with a summary of the properties of both Cyber Vision components. You can see below that the IP addresses are combined into one field to display both IPV4 and IPV6 IP addresses, and other properties like protocols are merged too.

Cisco Cyber Vision components aggregated in a single endpoint in ISE:



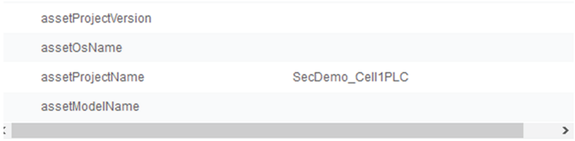
assetDeviceType	Engineering Station
assetId	2a90413b-36e8-5ad7-8963-516cf81132f1,e46a6ace-20e4-58b9-8b2f-7f8b3961ab77
assetIpAddress	fe80::e5b1:3cc0:4889:a2a3,192.168.0.44
assetMacAddress	00:0c:29:a5:06:9c
assetName	fe80::e5b1:3cc0:4889:a2a3,WORKSTATION-SIE
assetProtocol	IPv6,ARP, S7Discovery, Profinet, Profinet DCP, Profinet, S7Plus, ARP, Profinet DCP
assetVendor	VMware, Inc.
ip	fe80::e5b1:3cc0:4889:a2a3,192.168.0.44

4.2 Endpoints refresh

Cisco Cyber Vision sends components to ISE to create endpoints. When a new property is discovered on a component, it is sent to ISE and the endpoint is updated accordingly.

Example:

A Programmable Logic Controller (PLC) program project name has been discovered in Cisco Cyber Vision. It is pushed to ISE so the corresponding endpoint is updated:



assetProjectVersion	
assetOsName	
assetProjectName	SecDemo_Cell1PLC
assetModelName	

4.3 Properties supported

The following correlation table lists and describes all components properties that can be sent to ISE and their corresponding names.

ISE default properties are used, but some properties must be created manually in ISE (see in the table "ISE Custom Attributes: Yes").

CCV properties	Description	ISE properties	ISE Custom Attributes
ID	Cisco Cyber Vision Component ID	assetId	no
Name	Component name	assetName	no
Ip	Component IP address	assetIpAddress	no
Mac	Component MAC address	assetMacAddress	no
Vendor-name	Component manufacturer (IEEE OUI)	assetVendor	no
Model-ref	Manufacturer product ID	assetProductId	no

CCV properties	Description	ISE properties	ISE Custom Attributes
Serial-number	Manufacturer serial number	assetSerialNumber	no
Tags	All levels component tags are concatenated in one string	assetDeviceType	no
Fw-version	Component firmware version	assetSwRevision	no
Hw-version	Component hardware version	assetHwRevision	no
Protocols	All protocols are concatenated in one string	assetProtocol	no
Model-name	Manufacturer model name	assetModelName	yes
OS-name	Operating system name	assetOsName	yes
Project-name	Project name (inside PLC program)	assetProjectName	yes
Project-version	Project version (inside PLC program)	assetProjectVersion	yes
Group	Component group	assetGroup	yes
Group	Component group	assetCCVGrp	yes

All ISE Custom Attributes request policies in ISE to be refreshed. This configuration is described in this document.

5 Setup procedures

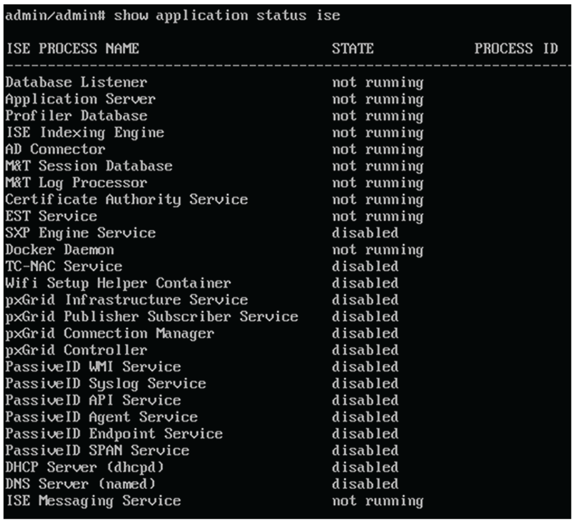
This section describes how to establish the link between ISE and Cisco Cyber Vision. To do so, you must perform the following procedures:

1. Enable pxGrid in ISE.
2. Customize ISE endpoint attributes.
3. Create ISE policies for Custom attributes.
4. Configure Cisco Cyber Vision to pxGrid communication.
5. Configure a custom host in ISE and the Cisco Cyber Vision Center if no DNS server is set for services.

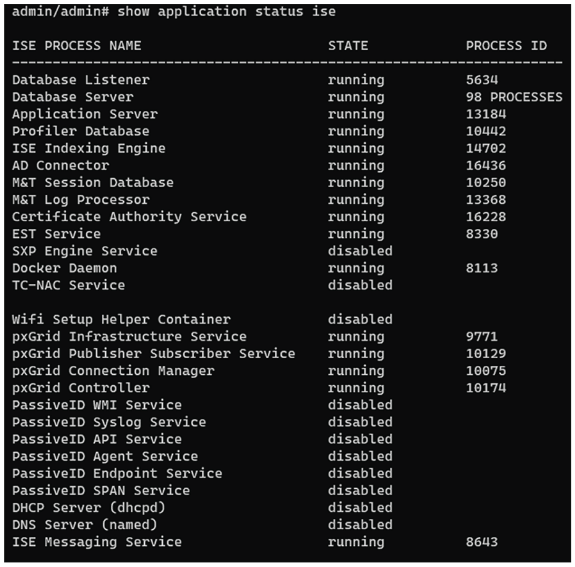
5.1 Enable pxGrid in ISE

To enable pxGrid in ISE:

1. Use the CLI to check all services are up and running.

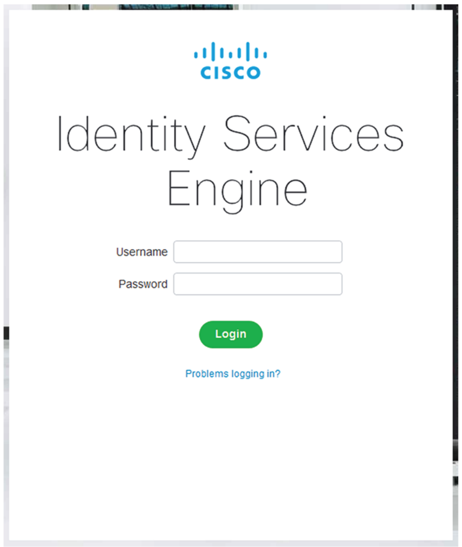


```
admin/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      not running
Application Server                     not running
Profiler Database                      not running
ISE Indexing Engine                    not running
AD Connector                           not running
M&T Session Database                   not running
M&T Log Processor                      not running
Certificate Authority Service          not running
EST Service                            not running
SXP Engine Service                     disabled
Docker Daemon                          not running
TC-NAC Service                         disabled
Wifi Setup Helper Container            disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  not running
```

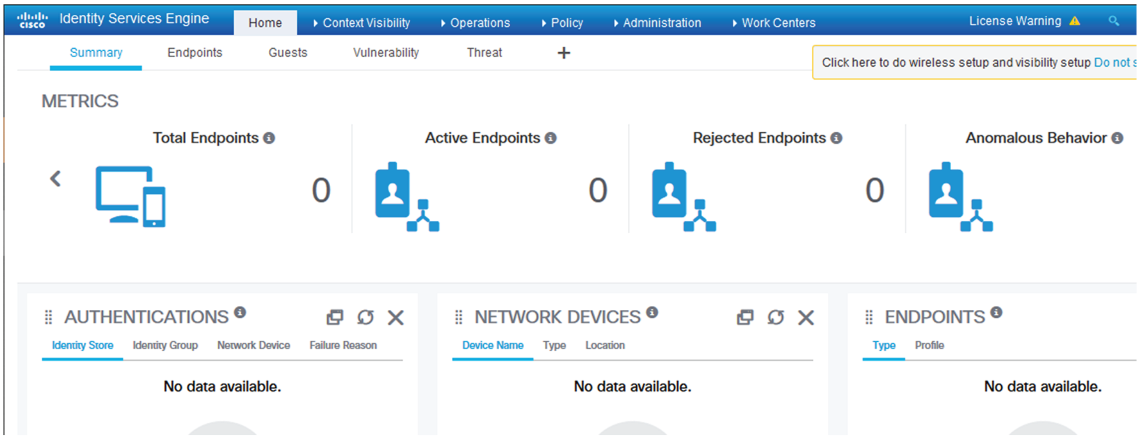


```
admin/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          5634
Database Server                        running          98 PROCESSES
Application Server                     running          13184
Profiler Database                      running          10442
ISE Indexing Engine                    running          14702
AD Connector                           running          16436
M&T Session Database                   running          10250
M&T Log Processor                      running          13368
Certificate Authority Service          running          16228
EST Service                            running          8330
SXP Engine Service                     disabled
Docker Daemon                          running          8113
TC-NAC Service                         disabled

Wifi Setup Helper Container            disabled
pxGrid Infrastructure Service          running          9771
pxGrid Publisher Subscriber Service    running          10129
pxGrid Connection Manager              running          10075
pxGrid Controller                      running          10174
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          8643
```

2. When ISE is ready, use the ISE administration node IP address in Firefox to reach the ISE's application.



3. Log in using an administrator account.
   The following screen appears:



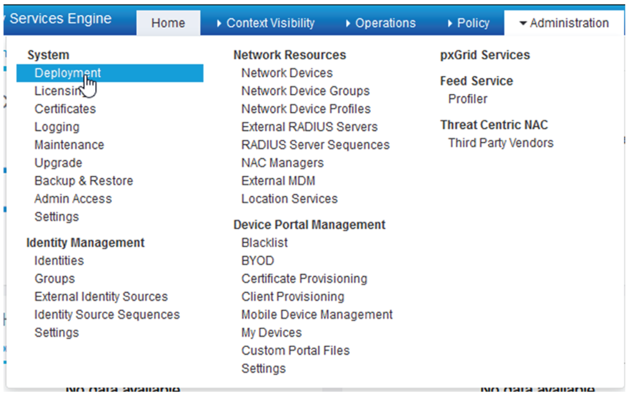
Click here to do wireless setup and visibility setup Do not s

No data available.

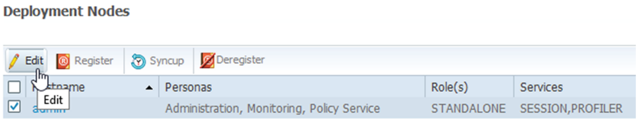
No data available.

No data available.

4. Navigate to Administration > System > Deployment.

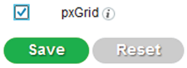


5. Click Edit under Deployment Nodes to set the properties of the ISE node where you want to activate pxGrid.

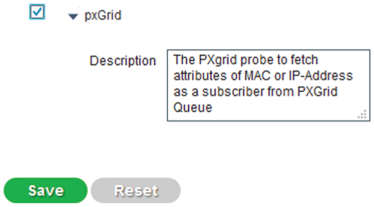

Deployment Nodes

	Hostname	Personas	Role(s)	Services
☑	admin	Administration, Monitoring, Policy Service	STANDALONE	SESSION,PROFILER

6. Under General Settings, select pxGrid and Save.

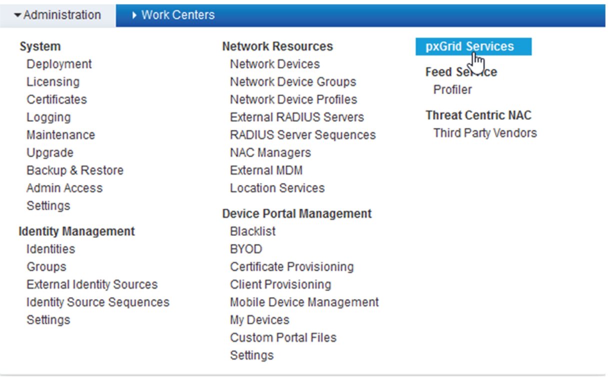

☑ pxGrid

7. Under Profiling Configuration, select pxGrid and Save.

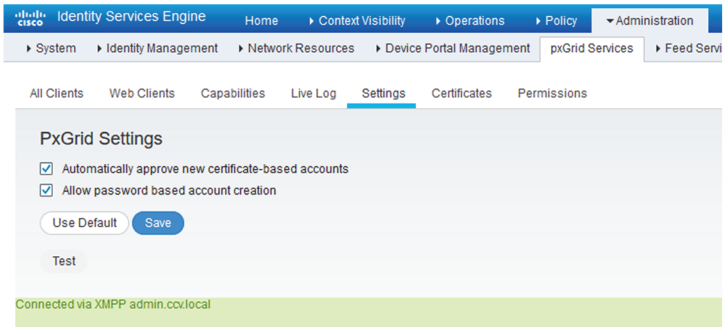

☑ pxGrid

Description: The PXgrid probe to fetch attributes of MAC or IP-Address as a subscriber from PXGrid Queue

8. Navigate to Administration > pxGrid Services.



9. Under Settings, select "Automatically approve new certificate-based accounts" and "Allow password based account creation", and Save.



PxGrid Settings

☑ Automatically approve new certificate-based accounts

☑ Allow password based account creation

Connected via XMPP admin.ccv.local

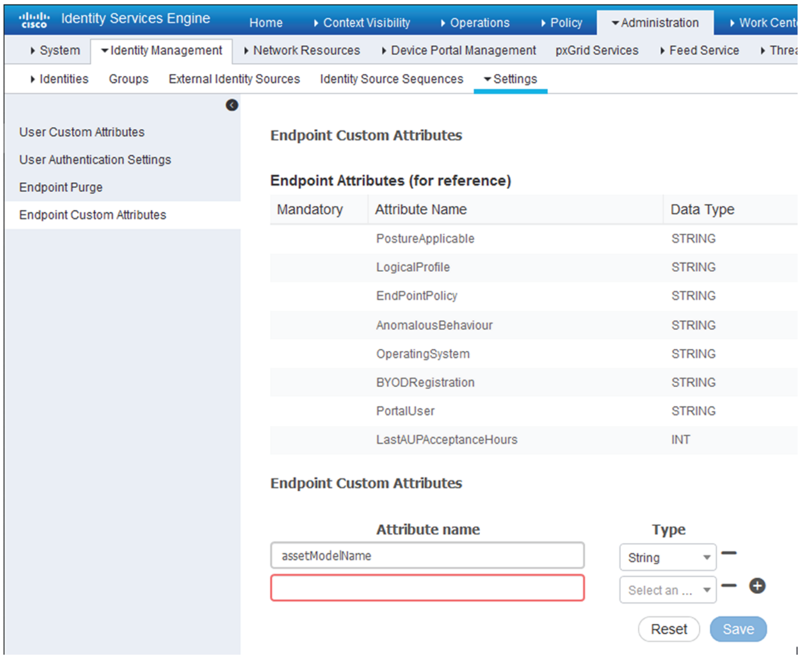
5.2 Customize ISE endpoint attributes

Before sending new endpoints to ISE, you must create the ISE Custom Endpoints Attributes listed below.

CCV properties	Description	ISE properties	ISE Custom Attributes
Model-name	Manufacturer model name	assetModelName	yes
OS-name	Operating system name	assetOsName	yes
Project-name	Project name (inside PLC program)	assetProjectName	yes
Project-version	Project version (inside PLC program)	assetProjectVersion	yes
Group	Component group	assetGroup	yes
Group	Component group	assetCCVGrp	yes

To create ISE Custom Endpoints Attributes:

1. Navigate to Administration > Identity Management > Settings > Endpoint Custom Attributes.



Endpoint Custom Attributes

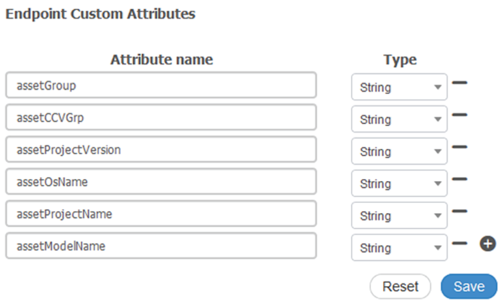
Endpoint Attributes (for reference)

Mandatory	Attribute Name	Data Type
	PostureApplicable	STRING
	LogicalProfile	STRING
	EndPointPolicy	STRING
	AnomalousBehaviour	STRING
	OperatingSystem	STRING
	BYODRegistration	STRING
	PortalUser	STRING
	LastAUPAcceptanceHours	INT

Endpoint Custom Attributes

Attribute name	Type
assetModelName	String
	Select an ...

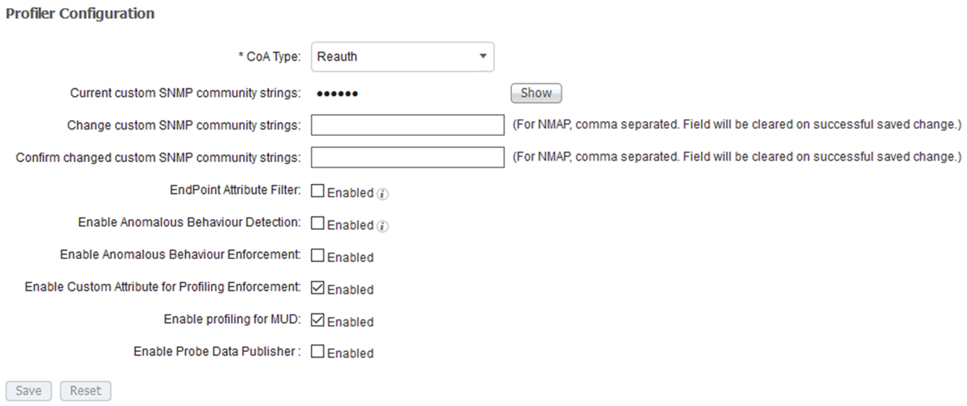
2. Use the form to create the Endpoints as shown below.
3. Select String as Type.
4. Click Save.



Endpoint Custom Attributes

Attribute name	Type
assetGroup	String
assetCCVGrp	String
assetProjectVersion	String
assetOsName	String
assetProjectName	String
assetModelName	String

5. Navigate to Administration > System > Settings > Profiling.
6. Under Profiler Configuration, select "Reauth" as CoA Type.
7. Select "Enable Custom Attribute for Profiling Enforcement" and "Enable profiling for MUD".



Profiler Configuration

* CoA Type:	Reauth
Current custom SNMP community strings:	•••••• Show
Change custom SNMP community strings:	(For NMAP, comma separated. Field will be cleared on successful saved change.)
Confirm changed custom SNMP community strings:	(For NMAP, comma separated. Field will be cleared on successful saved change.)
EndPoint Attribute Filter:	□ Enabled
Enable Anomalous Behaviour Detection:	□ Enabled
Enable Anomalous Behaviour Enforcement:	□ Enabled
Enable Custom Attribute for Profiling Enforcement:	☑ Enabled
Enable profiling for MUD:	☑ Enabled
Enable Probe Data Publisher :	□ Enabled

5.3 Create ISE policies for custom attributes

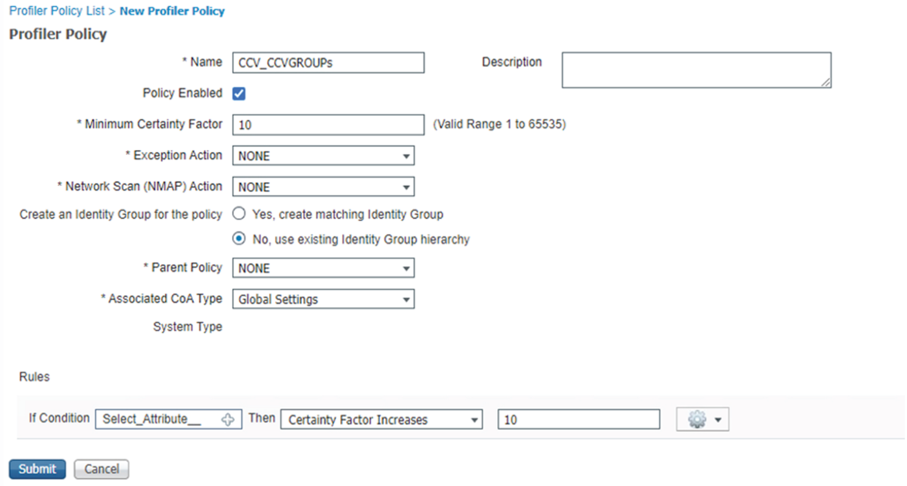
A policy must be created for each custom attribute to be updated by Cisco Cyber Vision.

The example below describes how to create a policy for the custom attribute "assetGroup".

To add a policy for the "assetGroup" attribute:

1. Navigate to Work Centers > Profiler > Profiling Policies.
2. Click Add.
3. Fill the form as shown below.

> **Note**
>
> Space character will not be accepted on the Name field. It should not be used or replaced by - or _.



Profiler Policy List > **New Profiler Policy**

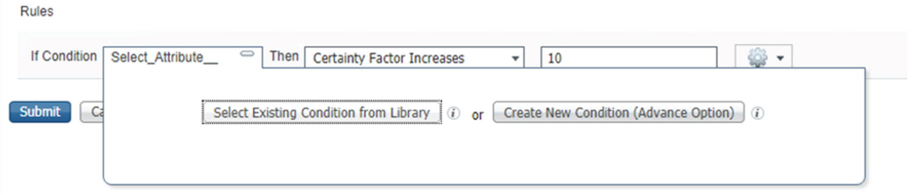
Profiler Policy

* Name: CCV_CCVGROUPs
Description:
Policy Enabled: ☑
* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)
* Exception Action: NONE
* Network Scan (NMAP) Action: NONE
Create an Identity Group for the policy: ○ Yes, create matching Identity Group ● No, use existing Identity Group hierarchy
* Parent Policy: NONE
* Associated CoA Type: Global Settings
System Type

Rules

If Condition: Select_Attribute__ Then: Certainty Factor Increases 10

4. Add a rule by clicking Select_Attribute and selecting Create New Condition (Advance Option).

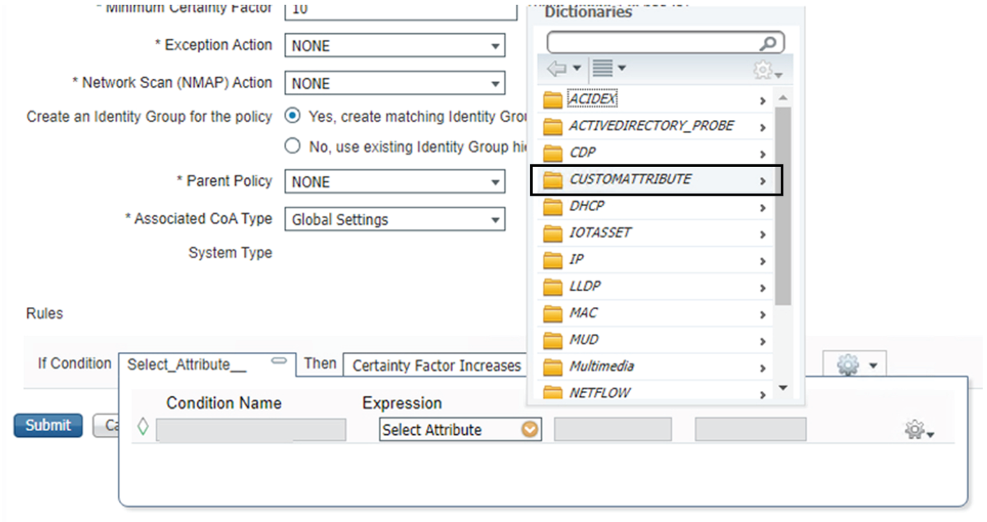


Rules

If Condition: Select_Attribute__ Then: Certainty Factor Increases 10

Submit
Ca
Select Existing Condition from Library
or
Create New Condition (Advance Option)

5. Under Expression, click Select Attribute, and select CUSTOMATTRIBUTE.



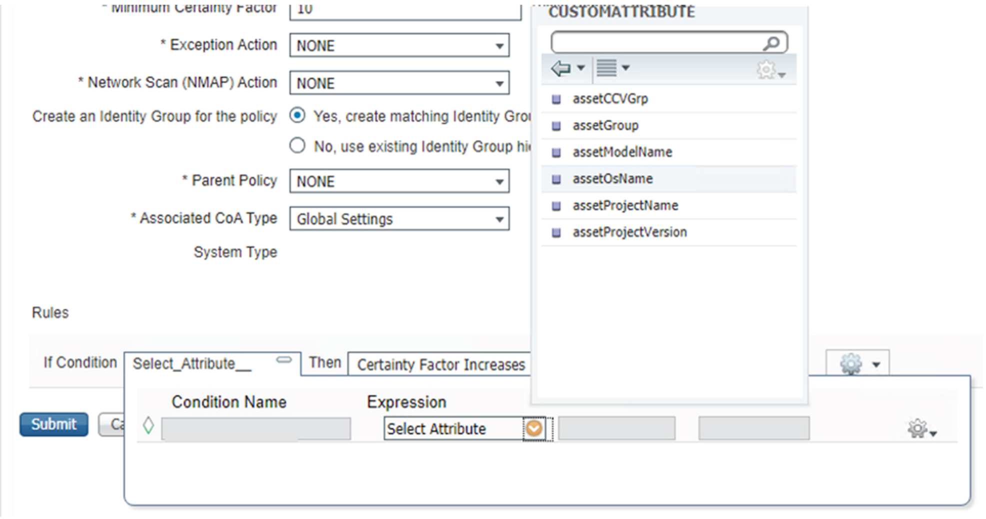
* Minimum Certainty Factor: 10
* Exception Action: NONE
* Network Scan (NMAP) Action: NONE
Create an Identity Group for the policy: ● Yes, create matching Identity Gro ○ No, use existing Identity Group hi
* Parent Policy: NONE
* Associated CoA Type: Global Settings
System Type

Rules

If Condition: Select_Attribute__ Then: Certainty Factor Increases

Condition Name | Expression: Select Attribute

6. Click assetGroup.



* Minimum Certainty Factor 10

* Exception Action NONE

* Network Scan (NMAP) Action NONE

Create an Identity Group for the policy ● Yes, create matching Identity Grou ○ No, use existing Identity Group hi

* Parent Policy NONE

* Associated CoA Type Global Settings

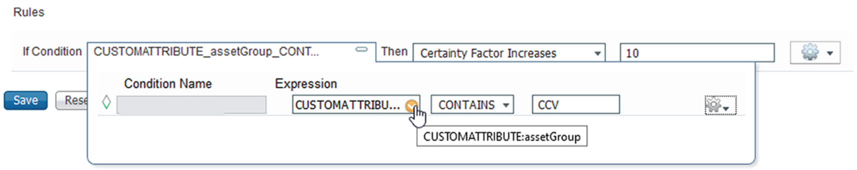
System Type

If Condition Select_Attribute__ Then Certainty Factor Increases

Expression: Select Attribute

- assetCCVGrp
- assetGroup
- assetModelName
- assetOsName
- assetProjectName
- assetProjectVersion

7. Fill the form as below by selecting CONTAINS and typing CCV.



If Condition CUSTOMATTRIBUTE_assetGroup_CONT... Then Certainty Factor Increases 10

Expression: CUSTOMATTRIBU... CONTAINS CCV

CUSTOMATTRIBUTE:assetGroup

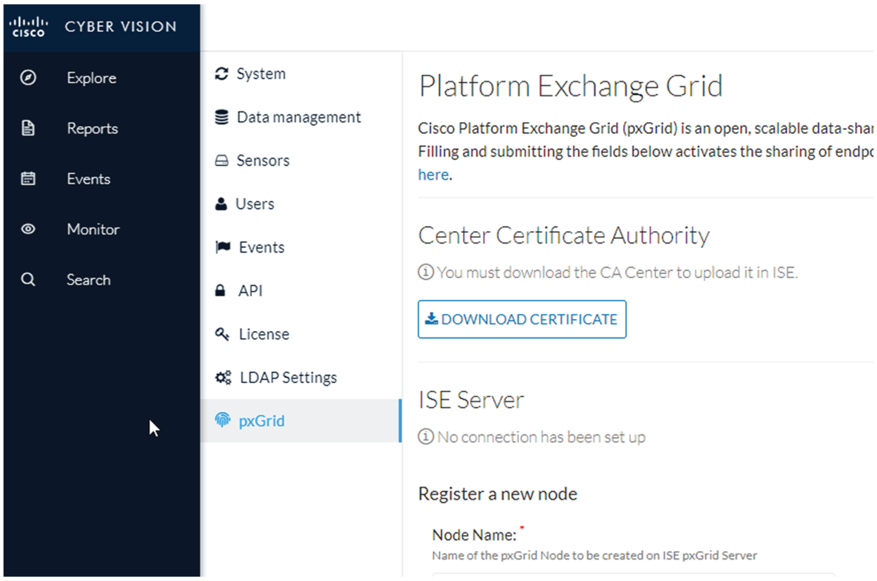
> **Note**
>
> All assetgroup values must be tested. An operator like CONTAINS or STARTWITH can be used to test several values.

8. Save the condition for the assetGroup condition and repeat the previous steps for each custom attribute.

5.4 Configure Cisco Cyber Vision to pxGrid communication

To retrieve Cisco Cyber Vision's Certificate Authority:

1. Access Cisco Cyber Vision application, and navigate to Administration > pxGrid.



Platform Exchange Grid

Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-shai
Filling and submitting the fields below activates the sharing of endpc
here.

Center Certificate Authority

You must download the CA Center to upload it in ISE.

ISE Server

No connection has been set up

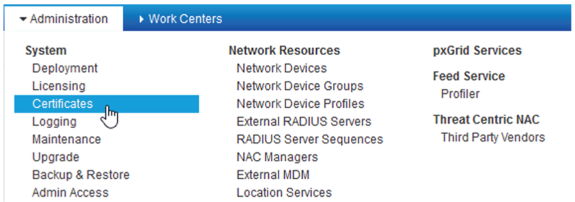
Register a new node

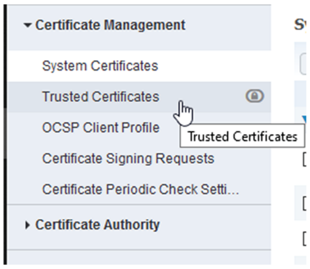
Node Name: *
Name of the pxGrid Node to be created on ISE pxGrid Server

2. Click the Download Certificate button to retrieve Cisco Cyber Vision's Certificate Authority.

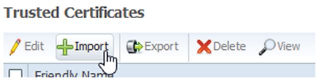
To import Cisco Cyber Vision's Certificate Authority in ISE and enable trust for authentication:

1. In ISE, navigate to Administration > Certificates > Certificate Management > Trusted Certificates.

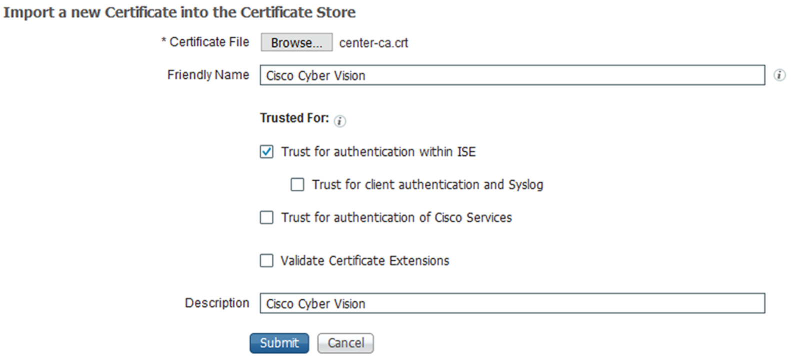




2. Click Import.



3. Click Browse and select Cisco Cyber Vision's Certificate Authority.
4. Give a name to the certificate.
5. Select "Trust for authentication within ISE".
6. Click Submit.


Import a new Certificate into the Certificate Store

* Certificate File: Browse... center-ca.crt

Friendly Name: Cisco Cyber Vision

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

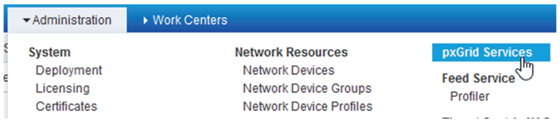
☐ Trust for authentication of Cisco Services

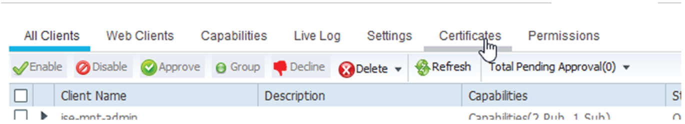
☐ Validate Certificate Extensions

Description: Cisco Cyber Vision

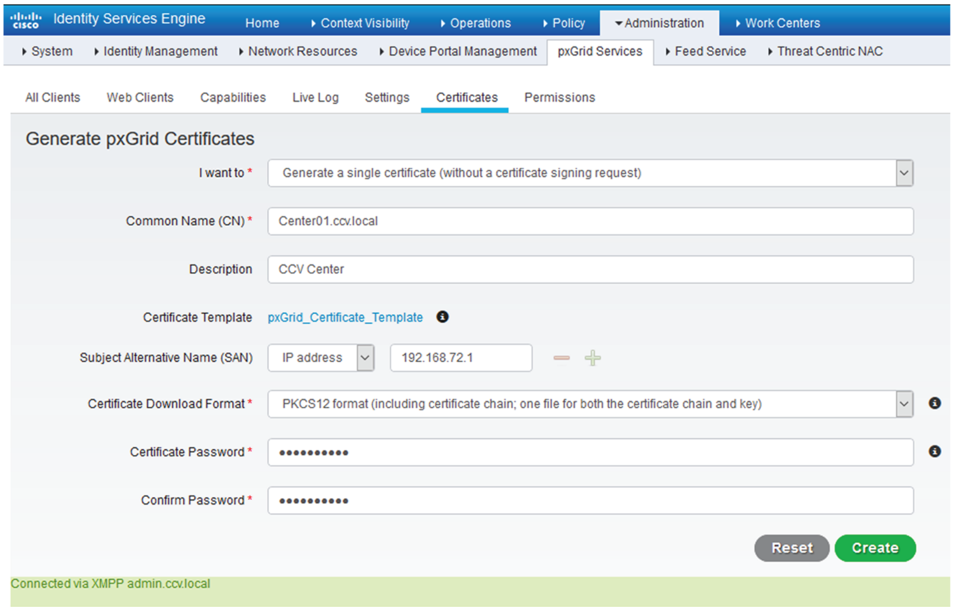
To generate a client certificate for Cisco Cyber Vision:

1. Navigate to Administration > pxGrid Services > Certificates.





2. Fill the form as shown below.



Generate pxGrid Certificates

I want to * Generate a single certificate (without a certificate signing request)

Common Name (CN) * Center01.ccv.local

Description CCV Center

Certificate Template pxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.72.1

Certificate Download Format * PKCS12 format (including certificate chain; one file for both the certificate chain and key)

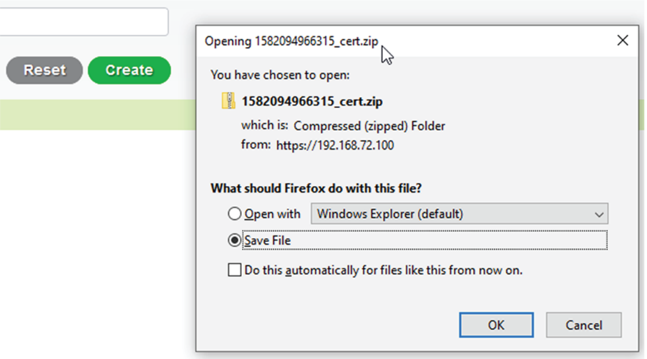
Certificate Password * ••••••••••

Confirm Password * ••••••••••

Connected via XMPP admin.ccv.local

> **Note**
>
> The CN field is mandatory because ISE CA is aimed to issue identity certificates. Ideally, Cisco Cyber Vision Center's FQDN should be entered, but since the identity certificate is not used by Cisco Cyber Vision, the CN field value is not critical.

3. Click the Create button to download the zip folder.



Opening 1582094966315_cert.zip

You have chosen to open:

1582094966315_cert.zip

which is: Compressed (zipped) Folder

from: https://192.168.72.100

What should Firefox do with this file?

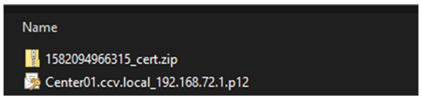
○ Open with Windows Explorer (default)

● Save File

□ Do this automatically for files like this from now on.

OK Cancel

4. Extract the files from the zip folder.

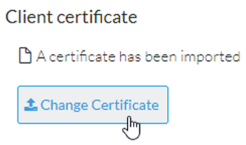


Name

1582094966315_cert.zip

Center01.ccv.local_192.168.72.1.p12

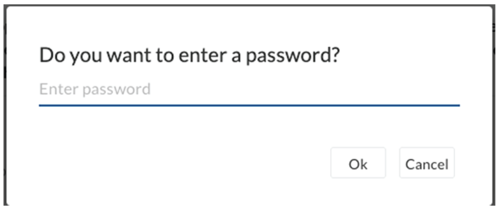
5. In Cisco Cyber Vision application, navigate to Administration > pxGrid, and click the Change Certificate button to upload the .p12 file.



Client certificate

A certificate has been imported

6. Type the password that was given during the certificate creation.

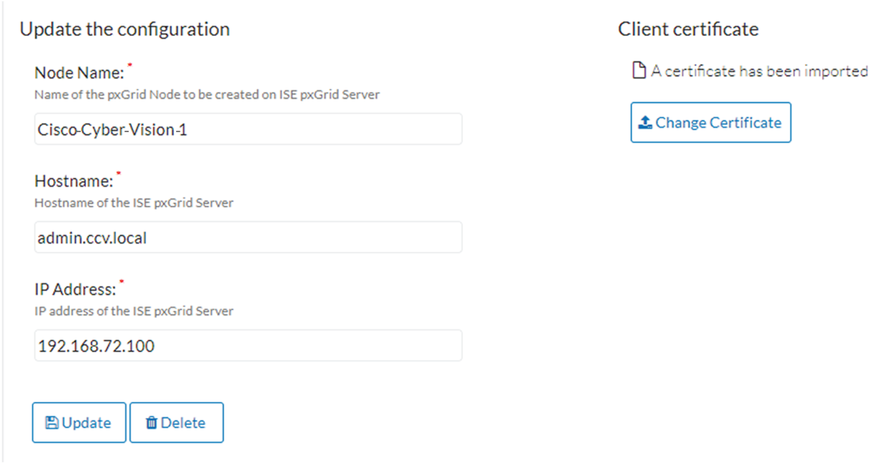


Do you want to enter a password?

Enter password

7. Fill in the fields as in the example shown below.

> **Note**
>
> Space character will not be accepted on the Node Name field. It should not be used or replaced by - or _.



Update the configuration

Node Name: *
Name of the pxGrid Node to be created on ISE pxGrid Server
Cisco-Cyber-Vision-1

Hostname: *
Hostname of the ISE pxGrid Server
admin.ccv.local

IP Address: *
IP address of the ISE pxGrid Server
192.168.72.100

Client certificate

A certificate has been imported

8. Click update.

5.5 Configure a custom host (optional)

If there is no DNS server for services, you may need to configure a custom host in the Cisco Cyber Vision Center and ISE so they can communicate.

To add the custom host in ISE and the Cisco Cyber Vision Center:

1. Add the custom host in ISE using the following commands:

```
ssh -c aes256-cbc admin@10.2.3.180
```

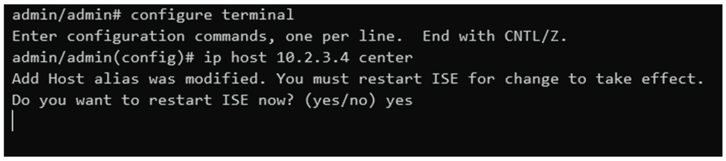
```
configure terminal
```

```
ip host 10.2.3.4 center
```

```
# wait for application to restart
```

```
End
```

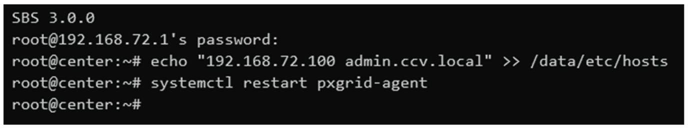
2. Type "yes" so ISE restarts.



```
admin/admin# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
admin/admin(config)# ip host 10.2.3.4 center
Add Host alias was modified. You must restart ISE for change to take effect.
Do you want to restart ISE now? (yes/no) yes
```

3. Add the custom host and restart pxgrid-agent in the Cisco Cyber Vision Center using the following commands:

```
ssh root@10.2.3.4
echo "10.2.3.180 ise.corp.sentryo.net" >> /data/etc/hosts
```



```
SBS 3.0.0
root@192.168.72.1's password:
root@center:~# echo "192.168.72.100 admin.ccv.local" >> /data/etc/hosts
root@center:~# systemctl restart pxgrid-agent
root@center:~#
```

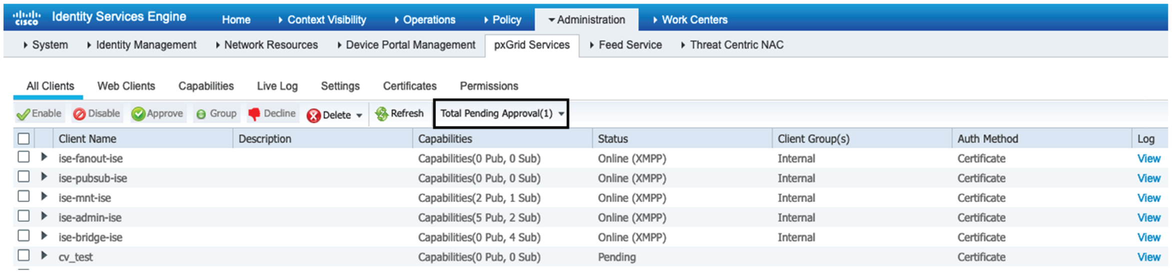
pxgrid-agent restarts automatically.

Wait a moment for both services to restart. Once it's done, approve Cisco Cyber Vision's request in ISE.

5.6 Approve the Cisco Cyber Vision request in ISE

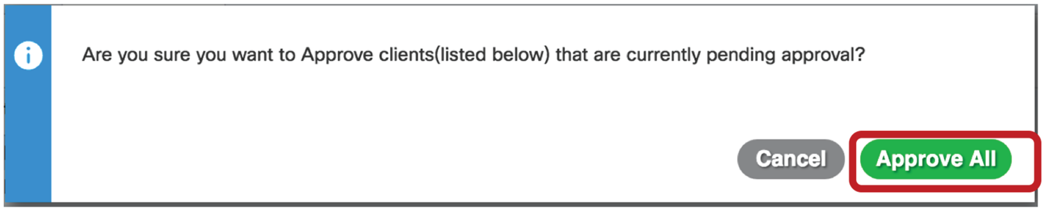
To approve the Cisco Cyber Vision request in ISE:

1. In ISE, navigate to Administration > pxGrid Services > All Clients.
   You should see a request for Pending Approval as Total Pending Approval(1).

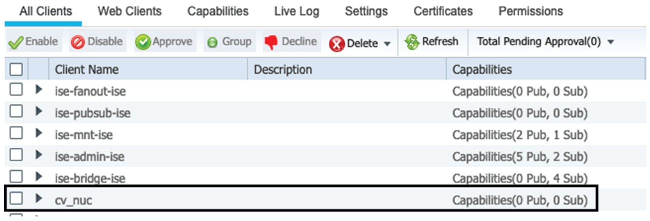


	Client Name	Description	Capabilities	Status	Client Group(s)	Auth Method	Log
□	ise-fanout-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-mnt-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-admin-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-bridge-ise		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
□	cv_test		Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View

2. Click Total Pending Approval(1) to see a drop down.
3. Click Approve All to approve the request from Cisco Cyber Vision.


Are you sure you want to Approve clients(listed below) that are currently pending approval?

You should see Cisco Cyber Vision on the list of clients as shown in the example below.

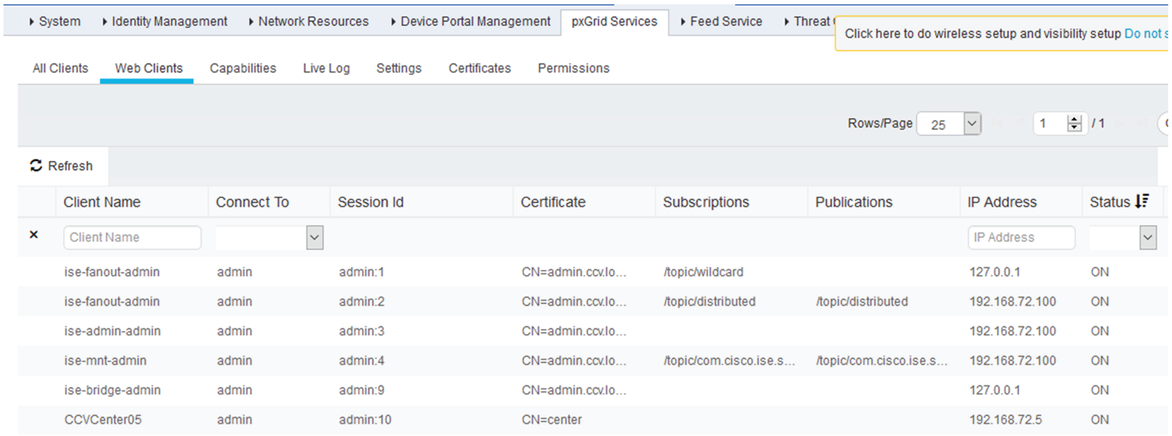


	Client Name	Description	Capabilities
□	ise-fanout-ise		Capabilities(0 Pub, 0 Sub)
□	ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)
□	ise-mnt-ise		Capabilities(2 Pub, 1 Sub)
□	ise-admin-ise		Capabilities(5 Pub, 2 Sub)
□	ise-bridge-ise		Capabilities(0 Pub, 4 Sub)
□	cv_nuc		Capabilities(0 Pub, 0 Sub)

The communication link should be established. To make sure of that, proceed with the following steps.

To check that the Center is visible in ISE:

In ISE, navigate to Administration > pxGrid services > Web clients. The Cisco Cyber Vision Center should appear in the client list.



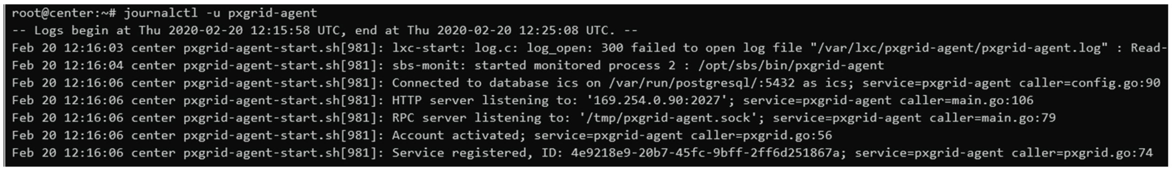
	Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status
×	Client Name						IP Address	
	ise-fanout-admin	admin	admin:1	CN=admin.ccv.lo...	/topic/wildcard		127.0.0.1	ON
	ise-fanout-admin	admin	admin:2	CN=admin.ccv.lo...	/topic/distributed	/topic/distributed	192.168.72.100	ON
	ise-admin-admin	admin	admin:3	CN=admin.ccv.lo...			192.168.72.100	ON
	ise-mnt-admin	admin	admin:4	CN=admin.ccv.lo...	/topic/com.cisco.ise.s...	/topic/com.cisco.ise.s...	192.168.72.100	ON
	ise-bridge-admin	admin	admin:9	CN=admin.ccv.lo...			127.0.0.1	ON
	CCVCenter05	admin	admin:10	CN=center			192.168.72.5	ON

To check the status in Cisco Cyber Vision:

1. Type in the Center's CLI the following command:

   ```
   journalctl -u pxgrid-agent
   ```

   The result should be like below:

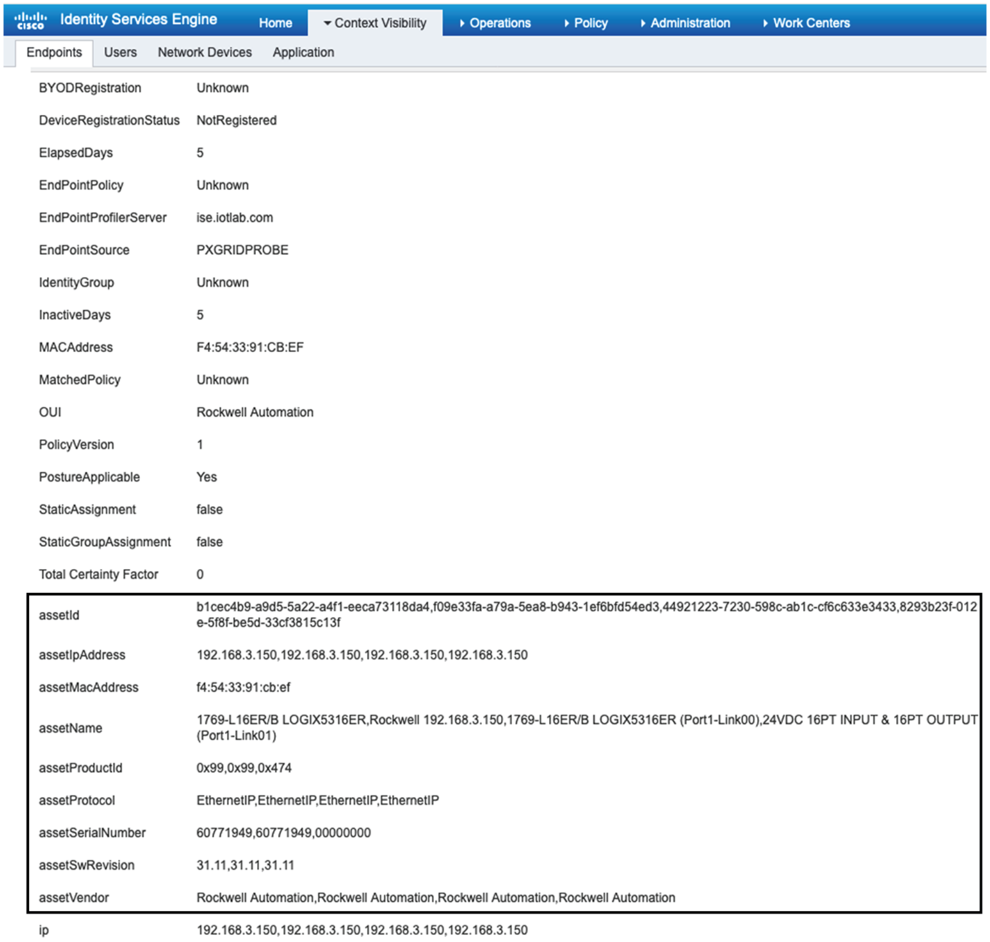


```
root@center:~# journalctl -u pxgrid-agent
-- Logs begin at Thu 2020-02-20 12:15:58 UTC, end at Thu 2020-02-20 12:25:08 UTC. --
Feb 20 12:16:03 center pxgrid-agent-start.sh[981]: lxc-start: log.c: log_open: 300 failed to open log file "/var/lxc/pxgrid-agent/pxgrid-agent.log" : Read-
Feb 20 12:16:04 center pxgrid-agent-start.sh[981]: sbs-monit: started monitored process 2 : /opt/sbs/bin/pxgrid-agent
Feb 20 12:16:06 center pxgrid-agent-start.sh[981]: Connected to database ics on /var/run/postgresql/:5432 as ics; service=pxgrid-agent caller=config.go:90
Feb 20 12:16:06 center pxgrid-agent-start.sh[981]: HTTP server listening to: '169.254.0.90:2027'; service=pxgrid-agent caller=main.go:106
Feb 20 12:16:06 center pxgrid-agent-start.sh[981]: RPC server listening to: '/tmp/pxgrid-agent.sock'; service=pxgrid-agent caller=main.go:79
Feb 20 12:16:06 center pxgrid-agent-start.sh[981]: Account activated; service=pxgrid-agent caller=pxgrid.go:56
Feb 20 12:16:06 center pxgrid-agent-start.sh[981]: Service registered, ID: 4e9218e9-20b7-45fc-9bff-2ff6d251867a; service=pxgrid-agent caller=pxgrid.go:74
```

To check Cisco Cyber Vision is sending endpoint attributes to ISE:

If Cisco Cyber Vision is sending device attributes, you should be able to find attributes in ISE endpoint attributes.

1. In ISE, navigate to Context Visibility > Endpoints.
2. Select an endpoint and look for attributes as shown below (those starting with asset such as assetName). These are the additional attributes supplied by Cisco Cyber Vision for industrial endpoints and can be used in ISE profiling policies.



BYODRegistration	Unknown
DeviceRegistrationStatus	NotRegistered
ElapsedDays	5
EndPointPolicy	Unknown
EndPointProfilerServer	ise.iotlab.com
EndPointSource	PXGRIDPROBE
IdentityGroup	Unknown
InactiveDays	5
MACAddress	F4:54:33:91:CB:EF
MatchedPolicy	Unknown
OUI	Rockwell Automation
PolicyVersion	1
PostureApplicable	Yes
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	0
assetId	b1cec4b9-a9d5-5a22-a4f1-eeca73118da4,f09e33fa-a79a-5ea8-b943-1ef6bfd54ed3,44921223-7230-598c-ab1c-cf6c633e3433,8293b23f-012e-5f8f-be5d-33cf3815c13f
assetIpAddress	192.168.3.150,192.168.3.150,192.168.3.150,192.168.3.150
assetMacAddress	f4:54:33:91:cb:ef
assetName	1769-L16ER/B LOGIX5316ER,Rockwell 192.168.3.150,1769-L16ER/B LOGIX5316ER (Port1-Link00),24VDC 16PT INPUT & 16PT OUTPUT (Port1-Link01)
assetProductId	0x99,0x99,0x474
assetProtocol	EthernetIP,EthernetIP,EthernetIP,EthernetIP
assetSerialNumber	60771949,60771949,00000000
assetSwRevision	31.11,31.11,31.11
assetVendor	Rockwell Automation,Rockwell Automation,Rockwell Automation,Rockwell Automation
ip	192.168.3.150,192.168.3.150,192.168.3.150,192.168.3.150

6 Troubleshooting

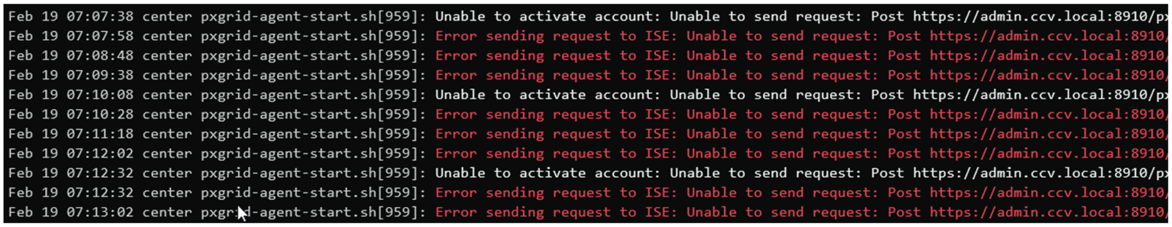
6.1 pxGrid agent logs

When the communication between Cisco Cyber Vision and ISE is not possible, the standard logs of pxgrid-agent will give an error like below.

To see these logs:

- Access the Cisco Cyber Vision Center's CLI in ssh and use the following command:

```
journalctl -u pxgrid-agent
```



```
Feb 19 07:07:38 center pxgrid-agent-start.sh[959]: Unable to activate account: Unable to send request: Post https://admin.ccv.local:8910/p
Feb 19 07:07:58 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
Feb 19 07:08:48 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
Feb 19 07:09:38 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
Feb 19 07:10:08 center pxgrid-agent-start.sh[959]: Unable to activate account: Unable to send request: Post https://admin.ccv.local:8910/p
Feb 19 07:10:28 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
Feb 19 07:11:18 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
Feb 19 07:12:02 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
Feb 19 07:12:32 center pxgrid-agent-start.sh[959]: Unable to activate account: Unable to send request: Post https://admin.ccv.local:8910/p
Feb 19 07:12:32 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
Feb 19 07:13:02 center pxgrid-agent-start.sh[959]: Error sending request to ISE: Unable to send request: Post https://admin.ccv.local:8910/
```

6.2 pxGrid agent and burrow advanced logs

To help you appreciate a potential issue in the ISE-Cisco Cyber Vision link, it is recommended to use the advanced logs of sbs-burrow and pxgrid-agent services. These logs can be requested by the product support.

To enable advanced logs, access the Cisco Cyber Vision Center's CLI in ssh and create two files in the folder /data/etc/sbs.

The first file must be named "listener.conf" and contain the following content:

```
# /data/etc/sbs/listener.conf
configlog:
loglevel: debug
```

The second file must be named "listener.conf" and contain the following content:

```
# /data/etc/sbs/pxgrid-agent.conf
configlog:
loglevel: debug
```

Once both files are created, reboot the Center, or restart the "sbs-burrow" and "pxgrid-agent" services.

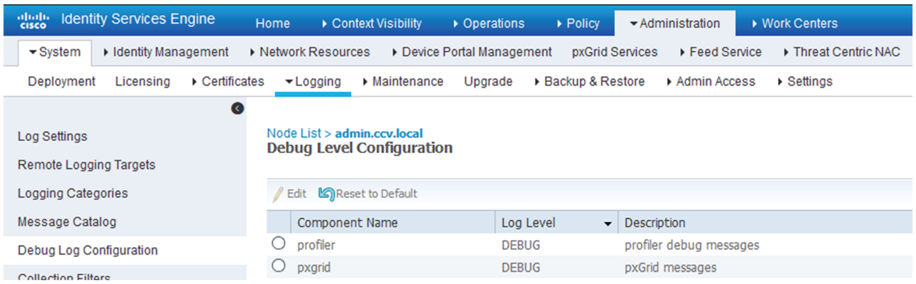
Restart a service using the following command:

```
systemctl restart <servicename>
```

6.3 Advanced logs in ISE

To see advanced logs, access ISE and navigate to:

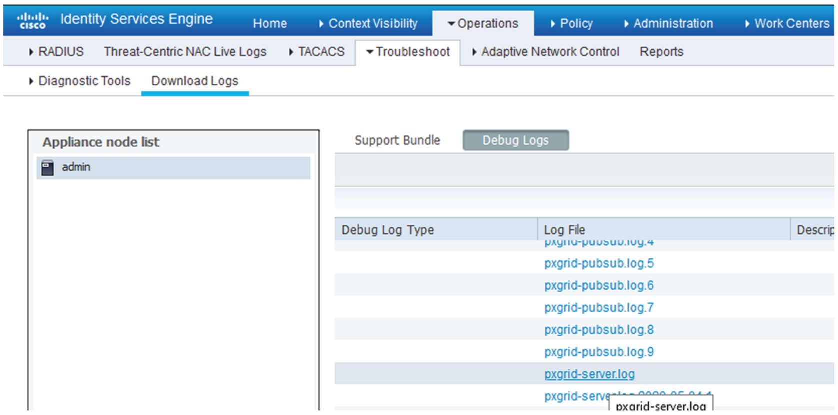
- Administration > Logging.



Node List > admin.ccv.local
Debug Level Configuration

	Component Name	Log Level	Description
○	profiler	DEBUG	profiler debug messages
○	pxgrid	DEBUG	pxGrid messages

- Operations > Download Logs.



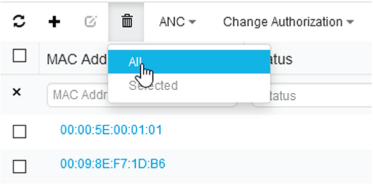
Debug Log Type	Log File	Descrip
	pxgrid-pubsub.log.4	
	pxgrid-pubsub.log.5	
	pxgrid-pubsub.log.6	
	pxgrid-pubsub.log.7	
	pxgrid-pubsub.log.8	
	pxgrid-pubsub.log.9	
	pxgrid-server.log	
	pxgrid-server.log.2020-05-04.1	

6.4 Delete endpoints in ISE (for test)

You can delete ISE's endpoints from the endpoint list for test purposes.

To do so:

1. Navigate to Context Visibility > Endpoints.
2. Click the Trash icon.
3. Select All.
4. Confirm the action.

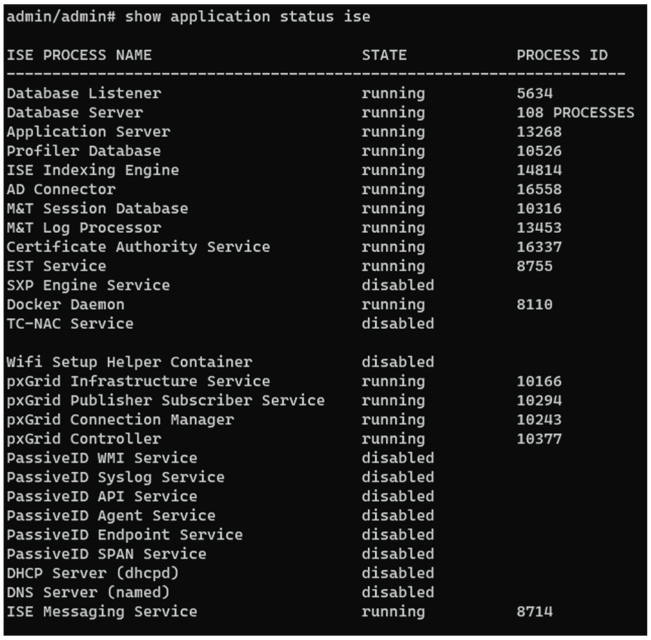


6.5 Check pxGrid status

- Check pxGrid status using the following command on ISE's CLI:

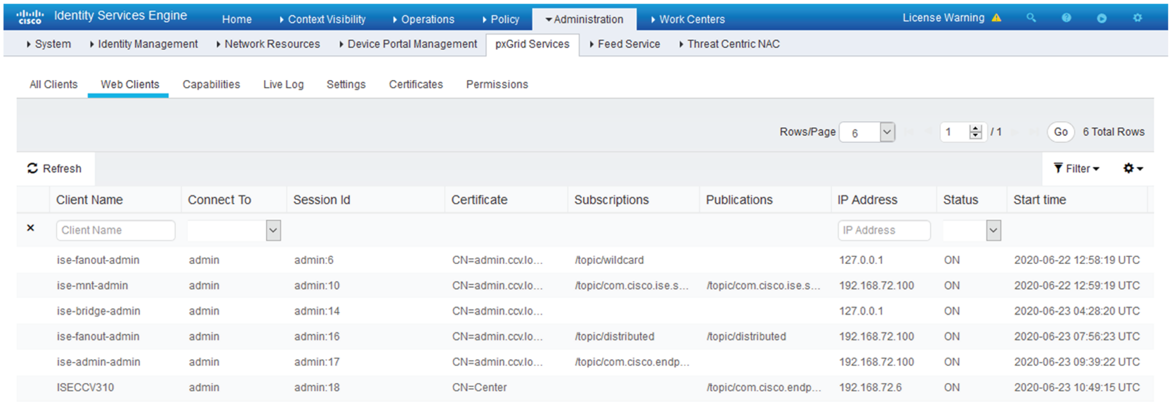
```
show application status ise
```

Results also include ISE status.



```
admin/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          5634
Database Server                        running          108 PROCESSES
Application Server                     running          13268
Profiler Database                      running          10526
ISE Indexing Engine                    running          14814
AD Connector                           running          16558
M&T Session Database                   running          10316
M&T Log Processor                      running          13453
Certificate Authority Service          running          16337
EST Service                            running          8755
SXP Engine Service                     disabled
Docker Daemon                          running          8110
TC-NAC Service                         disabled

Wifi Setup Helper Container            disabled
pxGrid Infrastructure Service          running          10166
pxGrid Publisher Subscriber Service    running          10294
pxGrid Connection Manager              running          10243
pxGrid Controller                      running          10377
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          8714
```

- Status can also be checked in the ISE application. To do so, navigate to Administration > pxGrid services.



Client Name	Connect To	Session Id	Certificate	Subscriptions	Publications	IP Address	Status	Start time
ise-fanout-admin	admin	admin:6	CN=admin.ccv.lo...	/topic/wildcard		127.0.0.1	ON	2020-06-22 12:58:19 UTC
ise-mnt-admin	admin	admin:10	CN=admin.ccv.lo...	/topic/com.cisco.ise.s...	/topic/com.cisco.ise.s...	192.168.72.100	ON	2020-06-22 12:59:19 UTC
ise-bridge-admin	admin	admin:14	CN=admin.ccv.lo...			127.0.0.1	ON	2020-06-23 04:28:20 UTC
ise-fanout-admin	admin	admin:16	CN=admin.ccv.lo...	/topic/distributed	/topic/distributed	192.168.72.100	ON	2020-06-23 07:56:23 UTC
ise-admin-admin	admin	admin:17	CN=admin.ccv.lo...	/topic/com.cisco.endp...		192.168.72.100	ON	2020-06-23 09:39:22 UTC
ISECCV310	admin	admin:18	CN=Center		/topic/com.cisco.endp...	192.168.72.6	ON	2020-06-23 10:49:15 UTC